

Acceptable Use Policy (AUP) for ELCAP Information Systems

Updated: 1st April 2011
Revision Date: 31st March 2012

Policy Statement

ELCAP wishes to ensure that its Information Systems are used responsibly and safely by all users. ELCAP must ensure that all data relating to individuals is kept confidential and secure. ELCAP therefore requires all users to use information systems including the internet, intranet and e-mail in a way that is legal, secure and confidential. All resources, including hardware, software and data remain the property of ELCAP and may not be changed without permission and must be returned when no longer required.

Procedure

All ELCAP 's IT facilities and information resources remain the property of ELCAP and not of any particular individual, team or department. By following this policy you will help ensure IT facilities are used:

- legally
- securely
- without undermining ELCAP
- effectively
- in a spirit of co-operation, trust and consideration for others
- so they remain available

The policy relates to all Information Technology facilities and services provided by ELCAP and includes specifically internet, intranet, e-mail, all databases, software applications and all equipment. Throughout the policy, these are referred to generally as IT resources.

This Acceptable Use Policy (AUP) applies to all company staff of ELCAP and to those others offered access to company resources.

Permitted use of IT Resources

The use of IT resources for personal use is permitted so long as it does not:

- Incur specific expenditure for ELCAP
- Impact on your performance of your job
- Is not within your working hours
- Break the law
- Bring ELCAP into disrepute

The use of IT resources may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.

The company reserves the right to access e-mail, Internet/intranet activity in the case of specific allegations of misconduct. The user shall be informed and any information obtained will not be disclosed wider than is absolutely necessary.

You should be aware that e-mail or Internet/intranet activity may be unavoidably read/accessed in the case of an authorized IT support technician resolving an IT issue. This information will not be disclosed to anyone except where there is a breach of the law or ELCAP guidelines.

The distribution of any information through the Internet, computer-based services, e-mail, and messaging systems is subject to the scrutiny of the company. The company reserves the right to determine the suitability of this information.

Precautionary and Disciplinary Measures

The company may suspend access to IT resources for any individual pending an investigation.

The company has the right and duty to report any illegal violations to the appropriate authorities. The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately.

Deliberate and serious breach of the policy statements will lead to disciplinary measures. Breaches of licensing and copyright agreements is illegal and may result in criminal charges

Internet

Use of the Internet by company employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the company and its business units. The Internet is to be used in a manner that is consistent with the company's standards of business conduct and as part of the normal execution of an employee's job responsibilities.

Users shall not:

- Visit Internet sites that contain obscene, hateful or other objectionable materials.
- Make or post indecent remarks, proposals, or materials on the Internet.

E-mail

Staff members may be offered an ELCAP email address to assist them in their business activities. An ELCAP email address is defined as any address that ends in 'elcap.org'.

- The company may attach a disclaimer to the end of any outgoing e-mail using the elcap.org domain name.
- Email is a formal means of communication. It should be treated in the same manner as a written letter or document.
- Offers and contracts made by email are legally binding.
- Postings by employees from an ELCAP email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ELCAP, unless posting is in the course of business duties.

Users shall not:

- Solicit e-mails that are unrelated to business activities or for personal gain.

- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Represent personal opinions as those of the company.
- Open an unsolicited attachment, even if it is from a recognized sender, unless you are certain that its contents are not harmful.
- Open or save an attachment with the suffix .exe, .pif, .com, .bat, .dll

Confidentiality

All computer processing of data relating to living individuals must be registered and be undertaken in accordance with ELCAPs data protection registration. Such processing may only be made on computers owned by ELCAP and located within the premises of ELCAP.

Unauthorised access is an offence under the Computer Misuse Act. If any user has gained access to information which should not be generally available then this should be reported to the IT Supervisor.

All files stored on removable media must be returned should you leave the organisation. Removable media includes, but is not restricted to: floppy disks; CDR/RW; DVD-R/RW; USB Keys; Flash media and DAT tapes.

Users shall not:

- Upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the company, or the company itself.
- Reveal or publicise confidential or proprietary information that includes, but is not limited to: financial information, new business and service ideas, marketing strategies and plans, databases and the information contained therein, customer lists, computer software source codes, computer/network access codes, and business relationships.

- Record or obtain information about individuals where to do so would be in breach of Data Protection¹.

Security

All passwords must be changed every 60 days

Users shall not:

- Disclose personal system passwords or other security details to any other staff, volunteer or external agent².
- Access system or network resources using another user's login.
- Leave a PC unattended without logging off.
- Download any software or electronic files without implementing virus protection measures that have been approved by the company.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.
- Examine, change, or use another person's files, output, or user name for which they do not have explicit authorisation.
- Install software without the permission of the IT Supervisor

Software

ELCAP must hold a valid licence for all software used.

The IT Supervisor is responsible for keeping proof of licences and original media.

All new software must be delivered to the IT Supervisor so that licences can be checked and the asset register can be updated. All software purchases must be approved by the IT Supervisor.

¹ Contact the HR Manager for further information on Data Protection.

² It may be necessary in certain circumstances to log on a user who does not have an account and has been authorised to access information and/or use system resources. You must not disclose your password to the user and should ensure that they are not unsupervised when logged in. If you suspect that another person knows your password, you must change it immediately.

New software should only be installed by the IT Supervisor or an approved IT technician.

Shareware, Freeware, Public Domain and Evaluation software is bound by the same policies and procedures as all software.

ELCAP will regularly audit all computers. This will be reconciled with our licences and any unlicensed or unauthorised software removed. Disciplinary action may be taken where unauthorised software is found.

Users shall not :

- Install software including screen savers, and/or use images, sound files or information where doing so is in breach of license agreements or copyright.
- Install games on corporate PCs.
- Store important information on local PC drives or removable media without ensuring that a copy is also stored on a network drive. Failure to do so will result in the information not being backed up centrally and will therefore be at risk.
- Perform any other inappropriate uses identified by the network administrator.
- Waste time on non-company business.

Hardware

All Hardware and Software purchases must be approved by the IT Supervisor

You must ensure that all equipment is used in accordance with its operating instructions.

No equipment should be dismantled or disassembled by anyone other than an authorised support technician.

No changes shall be made to the configuration and/or location of equipment or software without the prior consent of the IT Supervisor or authorised IT support.

Any equipment that is deemed to be unsafe or unfit for purpose must be reported to the IT Supervisor, or external maintenance company, immediately and should not be used until made safe.

Disposal of Equipment

The IT Supervisor is responsible for maintaining an inventory of all IT equipment.

No equipment will be disposed of or transferred from the organisation without the authorisation of the IT Supervisor.

Any equipment that is disposed of will have confidential information or copyright or licensed material removed, preferably by the removal and total destruction of the Hard Disk Drive.

Remote Access (working from home using VPN)

VPN configuration information and security settings must not be divulged to any other person. You must inform the IT Supervisor immediately if you believe that another person may have had access to this information.

The user is responsible for selecting an ISP, ensuring that their operating system software supports the VPN connection and for any associated costs or fees in relation to this.

The user must ensure that all critical security patches are applied to their operating system software and that this is maintained.

The user must ensure that they have an approved antivirus software solution and that this is kept up to date.

The user will be responsible for the configuration of their PC or laptop to establish the VPN connection.

Only approved VPN clients will be used.

Users will be disconnected after five minutes of inactivity. You must re-establish the connection again.

Artificial processes must not be used to maintain connection during periods of inactivity.

Only one VPN connection is allowed per PC / laptop.

If you dispose of or transfer a PC / laptop with VPN connection details configured on it, you must ensure that the connection settings are securely removed before hand. You must also notify the IT supervisor that the equipment has been disposed of or transferred. The IT supervisor will also advise you with regards the secure removal of ELCAP files from your hard disk drive.

Any company files taken from the server should only be stored temporarily on your local drive while you are working on the file or document. You must ensure that the revised file is then uploaded back on to the server and all copies securely removed from your local drive.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of ELCAP's network, and as such are subject to the same rules and regulations that apply to ELCAP owned equipment.

The logo for ELCAP is a large, light blue watermark. It features the word "ELCAP" in a serif font, centered within a large, stylized, light blue oval shape that has a swoosh-like appearance at the bottom.